IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicants:	Tsutomu MATSUMOTO et al.	Confirmation:	7204
Serial No.:	09/810,437	Group Art Unit:	2135
Filed:	March 19, 2001	Examiner:	H. Song
For.	CARD SETTLEMENT METHOD AND SYSTEM USING MOBILE INFORMATION TERMINAL		

REQUEST FOR RECONSIDERATION

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

August 6, 2007

Sir:

The following remarks are respectfully submitted in response to the Office Action mailed March 5, 2007, in the above-identified application, the period for response being extended two months to August 5, 2007.

Applicants thank the Examiner for the consideration given the present application and the courtesy extended Applicants' representative at the interview of August 2, 2007. At the interview, the Examiner expressed support for Applicants' arguments in support of patentability. In addition, the Examiner agreed to withdraw the outstanding rejection of the claims and to allow the present application, contingent upon the filing of a formal response consistent with the discussion at the interview and the Examiner's conducting another search.

In the Office Action pending claims 1, 4-6, 9, 10, and 15-20 are rejected under 35 U.S.C. §103(a) over Maes et al. (U.S. 6,016,476) in view of Gifford (U.S. 6,205,437 and U.S. 2001/0037308), and Pathmasuntharan et al. (U.S. 6,955,299). For the record, Applicants traverse and respectfully request reconsideration of this rejection.

In a first embodiment shown in FIG. 4, the present invention provides a method of settling a transaction that begins in step 1 by connecting the user terminal (10) and the authorization server (22) of the service center (20). In step 2, the authorization center (22) authenticates the IC card (4). In step 3, the identity of the user is verified by the authorization center (22) through the entry of a personal identification number (PIN). In step 4, the user enters the PIN. In step 5, IC credit or debit card information is transmitted to the settlement server (41) of the card company/bank (40). In step 6, the settlement server generates a one-time password usable for only one transaction and useable for a limited period of time. In step 7, the user then inputs the one-time password as displayed on the mobile telephone (1) into the CAT terminal of debit terminal (30) of the business establishment. In step 8, the CAT terminal or debit terminal (30) transmits the one-time password to the settlement server (41). Finally, in step 9, the settlement server (41) transfers the data to the CAT or debit terminal necessary to settlement of the transaction.

Maes describes a portable client PDA having I/O capability to read a smart card. The PDA also has a radio frequency modem for communications. The PDA can operate in

a client/server mode in which a temporary digital certificate is periodically downloaded to the PDA. This temporary digital certificate is used to access information stored in PDA and to write such information to the Universal smart card. Once the information is written to the smart card, a transaction may take place.

Maes further describes a smart card reader and writer built into a cellular telephone. At column 5, lines 25-27, Maes states:

> The PDA device 10 includes a smartcard reader/writer 26 (as is known in the art) for reading and writing information to and from various cards, e.g., magnetic cards, IC cards...

At column 14, lines 12-13, Maes indicates that "the functions and components of the PDA device 10 may be built into a cellular phone."

Gifford describes a system for purchasing goods or information over a computer network. Payments may be made based on a secret function of payment order parameters, ***a single-use transaction identifier***, or a specified network address.

Pathmasuntharan uses both a contact type IC card and a non-contact type IC card built into the mobile telephone. At column 1, lines 42-50, Pathmasuntharan states:

> Alternatively, a user may place the smart card (for a contact-less smart card) in front of the smart card reader, and the smart card exchanges electronic cash value information with the smart card reader by using radio frequency (RF) signals to perform the transaction. If the appropriate electronic cash value information is exchanged, the smart card reader and the smart card perform the transaction for the purchase of goods or services.

Whereas Pathmasuntharan appears to disclose the use of contact- and non-contact-type IC cards for the purchase of goods and services, the Office Action does not address the limitation "wherein the temporary password is data obtained by ***encrypting*** said settlement information and said temporary password is ***not*** stored in said settlement server." In fact, none of the references relied on in the Office Action discloses or suggests creating a one-time use temporary password using settlement information and the password not being stored in the settlement server.

In contrast, at page 14, line 37, through page 15, line 2, the present specification specifically indicates that the "password itself is data obtained by encrypting the above settlement information, the password itself is not stored at the settlement server."

Earlier, at page 4, lines 3-6, the specification described the settlement information as "containing at least a card number, and personal identification information input from the customer and proving the legitimacy of the customer."

Clearly, Maes teaches away from Applicants' claimed invention. Note column 7, lines 20-35, where Maes states:

> Enrollment also involves providing the service provider with personal information such as the user's social security number, address, maiden name and date of birth, which is ***stored on the central server 60***. Such information is then used to verify the user during the client/server mode prior to the issuance of a digital certificate. A personal identification number PIN and the Universal Card 26 with a unique account number 27 is provided by the service provider. This information, as well as biometric data such as voice prints (models) of the user, are also stored in central server 60 of the service provider for user verification during the client/server mode to obtain a digital certificate (to be discussed in detail below). ***The central server 60 is a computer which is programmed to perform the functions described herein***

> ***such as biometric verification, speech recognition and generating and downloading a temporary digital certificate.*** (emphasis added)

In view of the foregoing remarks, which are consistent with the discussion at the interview, reconsideration and withdrawal are requested of the rejection of claims 1, 4-6, 9, 10, and 15-20 as being obvious over Maes in view of Gifford and Pathmasuntharan et al. (U.S. 6,955,299).

Applicants hereby request a two-month extension of time in which to file this response and hereby authorize the Commissioner to charge any required fee not otherwise paid, including application processing, extension, and extra claims fees, to Deposit Account 01-2340.

Respectfully submitted,
KRATZ, QUINTOS & BROOKS, LLP

By: Charles Kratz Jr : Reg No. 22,631

for: George N. Stevens, #36,938

Docket No. 010369
1420 K Street, NW, Suite 400
Washington, DC 20005
(202) 659-2930

23850
PATENT TRADEMARK OFFICE

GNS:rk

Certificate of Transmission: I hereby certify that this correspondence is being transmitted via telecopier to the U.S. Patent and Trademark Office on August 6, 2007.

Roseanna Kaplan